U.S. General Services Administration

EIS and Zero Trust Architecture

How are you progressing on your Zero Trust Architecture journey?

Highlights

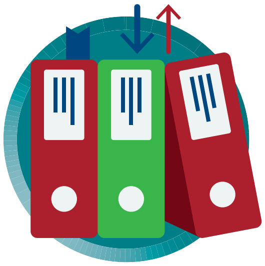
GSA's Enterprise Infrastructure Solutions (EIS) industry partners can help agencies with the planning and implementation of their Zero Trust Architecture (ZTA) solutions in alignment with the goals of the Executive Order 14028, Improving the Nation's Cybersecurity [Sec. 3 (a – c)].

EIS ZTA solution sets are consistent with:

- The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 description of ZTA
- The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model
- Office of Management and Budget (OMB) Memorandum M-19-26, Update to Trusted Internet Connections (TIC) Initiative

EIS is an ideal contract vehicle to plan, implement, and operationally support the logical components of your ZTA deployment.

How to Get It



EIS services such as the Software-Defined Wide Area Network Service (SDWANS), Managed Security Services (MSS), Managed Network Services (MNS), Managed Mobility Services (MMS), and the cloud services (IaaS, PaaS, SaaS) can provide the logical components and ongoing operational support of a ZTA.

Other GSA contracts, such as the Multiple Award Schedule (MAS) and Governmentwide Acquisition Contracts (GWACs), can also support integrated or managed ZTA solutions.

GSA published the "**Zero Trust Architecture (ZTA) Buyer's Guide**" to help agencies.

Business Value

The tenants of a ZTA as noted in NIST SP 800-207 are instrumental in identifying and managing cybersecurity risks.

Implementing a ZTA will help agencies access the benefits of cloud computing and shared services while increasing security and potentially lowering overall cost.

Implementing elements of a ZTA will improve user experiences by enabling direct access to the internet and to cloud resources while optimizing data-access traffic patterns and preventing bottlenecks.

EIS industry partners can directly help with agency planning, implementation, and continued operational support of the logical components of a ZTA solution by leveraging EIS managed-service offerings.

SD-WAN pricing models indicate significantly lower total cost of network management with centralized control and orchestration.

Recommendations

Reach out to your GSA Solutions Broker to engage GSA resources for help with reviews of your current architecture to identify areas for modernization – and for solicitation advice to leverage GSA tools, products, and services.

Review the CISA Zero Trust maturity model and the NIST SP 800-207 description of ZTA.

Ensure the solutions address CISA's five distinct ZTA pillars: Identity, Device, Network, Application Workload, and Data.

EIS Services Enabling ZTA

The following EIS services may be combined to obtain components of Zero Trust Architecture solution sets.

- SDWANS and Underlay (transport and access)
- Managed Security Service (MSS)
- Managed Network Service (MNS)
- Managed Mobility Service (MMS)
- Cloud Services IaaS, PaaS, SaaS
- Service Related Equipment (SRE)
- Service Related Labor (SRL)

Software-Defined Wide Area Network Service (SDWANS) – Implement managed or co-managed SD-WANS as an "overlay" to better enable the logical components of a ZTA and several of the TIC 3.0 Use Cases. Multiple "underlay" transport and access (e.g., Internet Protocol Service [IPS], broadband internet, mobile wireless) can be utilized for increased availability.

Managed Security Services (MSS) – Comprehensive cybersecurity solutions such as Cloud Access Security Brokers (CASB), Identity and Access Management, Endpoint Management, Secure Web Gateway, Trusted Internet Connections (TIC).

Managed Network Services (MNS) – Network planning, design, implementation, maintenance, operations, and customer service.

Cloud Services – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are FedRAMP-authorized cloud-based solutions.

Managed Mobility Services (MSS) – Manage mobile devices, wireless networks, and other mobile computing services.

Service Related Equipment (SRE) – Equipment required to fully deploy an EIS service.

Service Related Labor (SRL) – EIS network services already include all service-related labor necessary to implement the services. However, in a task order for procuring one or more network services, an agency may opt to include additional labor to support the EIS services.

EIS Services Enabling ZTA

Examples of how EIS services may be combined to support components of certain Zero Trust Architectures.

Example 1 – TIC 3.0 Remote User Use Case solutions – Improve productivity and user experience of remote workers with secure and optimized paths to the internet, cloud service providers, and agency internal resources

Managed Security Service (MSS) + Managed Network Service (MNS) + Managed Mobility Service (MMS) + Service Related Labor (SRL)

Example 2 – Secure Access Service Edge (SASE) – a network architecture that combines VPN and SD-WAN capabilities with cloud-native security functions such as secure web gateways, cloud access security brokers, firewalls, and zero-trust network access.

SDWANS and Underlay (transport and access) + Managed Security Service (MSS) + Managed Network Service (MNS) + Cloud Services IaaS, PaaS, SaaS + Service Related Equipment (SRE) + Service Related Labor (SRL)

Example 3 – Cloud Access Security Broker (CASB) – cloud-hosted software that act as a policy enforcement point between users and cloud service providers.

Managed Security Service (MSS) + Cloud Service SaaS + Service Related Labor (SRL)

For More Information

Contact your designated GSA representative via **www.gsa.gov/nspsupport** or call 855-482-4348.

www.gsa.gov
September 2021
05-21-01216

View, download, and order publications via www.gsa.gov/cmls.